# THE INFIMUM, SUPREMUM AND GEODESIC LENGTH OF A BRAID CONJUGACY CLASS

JOAN S. BIRMAN[1], KI HYOUNG KO[2], AND SANG JIN LEE

Abstract. Algorithmic solutions to the conjugacy problem in the braid groups $B_n, n = 2, 3, 4, \ldots$ were given in [3] and in [1]. This note concerns the computation of two integer class invariants, known as 'inf' and 'sup'. A key issue in both algorithms is the number $m$ of times one must 'cycle' (resp. 'decycle') in order to either increase inf (resp. decrease sup) or to be sure that it is already maximal (resp. minimal) for the class. Our main result is to prove that $m$ is bounded above by $((n^2-n)/2)-1$ in the situation of [3] and by $n-2$ in the situation of [1]. It follows immediately that the computation of inf and sup is polynomial in both word length and braid index, in both algorithms. The integers inf and sup determine (but are not determined by) the shortest geodesic length for elements in a conjugacy class, as defined in [2], and so we also obtain a polynomial-time algorithm for computing this length.

March 21, 2000

## 1. Introduction

The conjugacy problem in the $n$-string braid group $B_n$ is the following decision problem:

> Given two braids $\alpha, \alpha' \in B_n$, determine, in a finite number of steps, whether $\alpha = \gamma\alpha'\gamma^{-1}$ for some $\gamma \in B_n$.

In the late sixties Garside [4] solved the (word and) conjugacy problems in $B_n$. His solution to both problems was exponential in both word length and braid index. Subsequently, the efficiency of his algorithm was improved by Thurston [7] and Elrifai-Morton [3] to give a solution to the word problem which is polynomial in both word length and braid index.

All three papers [4], [7] and [3] work with the following well-known presentation of $B_n$, which we will call the *old presentation*:

[1] PARTIALLY SUPPORTED BY NSF GRANTS DMS-9705019 AND DMS-9973232.

[2] THE AUTHOR WISHES TO ACKNOWLEDGE THE FINANCIAL SUPPORT OF THE KOREA RESEARCH FOUNDATION MADE IN THE PROGRAM YEAR OF 1999

$$\begin{array}{ll} \text{generators:} & \sigma_1, \dots, \sigma_{n-1} \\ \text{relations:} & \sigma_i\sigma_j = \sigma_j\sigma_i, \quad |i-j| > 1 \\ & \sigma_i\sigma_j\sigma_i = \sigma_j\sigma_i\sigma_j, \quad |i-j| = 1 \end{array}$$

There is also a parallel and slightly more efficient solution to the word and conjugacy problems in [1], due to the authors of this paper. It uses a different presentation which we call the *new presentation*:

$$\begin{array}{ll} \text{generators:} & a_{ts}, \quad n \geq t > s \geq 1 \\ \text{relations:} & a_{ts}a_{rq} = a_{rq}a_{ts}, \quad (t-r)(t-q)(s-r)(s-q) > 0 \\ & a_{ts}a_{sr} = a_{tr}a_{ts} = a_{sr}a_{tr}, \quad n \geq t > s > r \geq 1 \end{array}$$

The terms *old* and *new* are due to Krammer, who used the new presentation in [6]. Both the old and new solutions to the word problem are polynomial in word length and braid index, but the best estimates obtained for the complexity of the solution to the conjugacy problem (see [1]) were rough exponential bounds. It was clear that better answers could not be obtained without more detailed information about the combinatorics, using either the old or new presentation.

Let $|W|$ denote the letter length of $W$, as a word in the given set of generators of $B_n$. The main result in this note is an algorithm which is polynomial in both $|W|$ and $n$ for computing two key integer invariants of the conjugacy class $[W]$ of $W$. The invariants in question are known as the *infimum* and *supremum* (or more informally *inf* and *sup*), using either presentation. See §2 below for precise definitions. We will also be able to compute the *geodesic length* (defined in §2,4 below) for the conjugacy class in polynomial time.

The reason we are able to do this requires some explanation. The method for finding *inf* (resp. *sup*) in both [3] and [1] rests on a procedure which is known as *cycling* (resp. *decycling*). While cycling and decycling are clearly finite processes, it had not been known how many times one must iterate them to either increase $\inf(W')$ (resp. decrease $\sup(W')$) for a word $W' \in [W]$ or to guarantee that a maximum (resp. minimum) value, denoted by $\inf([W])$ (resp. $\sup([W])$), for the conjugacy class has already been achieved. For the old presentation it had been claimed in [7] that the bound is 1, however an example was given in [3] for which 2 cyclings were needed to increase the infimum. Up to now, there were no published results which gave bounds, except for a very crude estimate in [1]. Our main result in this note is to find upper and lower bounds for the number of times one must cycle (resp. decycle), using either presentation, in order to replace a given word $W$ with $W' \in [W]$, where $\inf(W') > \inf(W)$ (resp. $\sup(W') < \sup(W)$), or be sure that $W$ realizes $\inf([W])$ (resp. $\sup([W])$). For the new

presentation we will prove that our upper bound is the best possible one.

Here is an outline of this paper. In §2 we review the background and state our results in a precise way. See Theorem 1, Corollary 2 and Corollary 3. In §3, we prove these three results. In §4, we give examples which prove that the bound in Corollary 2 is sharp for the new presentation, with somewhat weaker results for the old. In §5 we discuss the open problem of whether the solutions which we know to the conjugacy problem are polynomial in word length and braid index, and state several conjectures relating to that matter and also to the 'shortest word problem' in $B_n$, defined in that section.

## 2. **Statement of Results**

In this section we state our results precisely. To do so we need to review what has already been done. Since almost all the machinery is identical in the two theories, it will be convenient to introduce unified notation, so that we may review both theories at the same time. The symbol $W$ will be used to indicate a word in the generators of $B_n$, using either presentation. The element and conjugacy class which $W$ represents will be denoted $\{W\}$ and $[W]$. The letter length of $W$ is $|W|$.

2.1 Note that the relations in the old and new presentations are equivalences between positive words with same word-length. So the word-length is easy to compute for positive words. Let $B_n^+$ be the semigroup defined by the same generators and relations in the given presentation. The natural map $B_n^+ \to B_n$ is injective. [4, 1].

2.2 There is a *fundamental braid* $\mathbf{D}$. In the old presentation, $\mathbf{D}$ has length $((n^2-n)/2)-1$ and is the half-twist

$$\Delta = (\sigma_1 \cdots \sigma_{n-1})(\sigma_1 \cdots \sigma_{n-2}) \cdots (\sigma_1\sigma_2)\sigma_1.$$

In the new presentation it has length $n-1$ and it is the $(1/n)$-twist

$$\delta = a_{n(n-1)}a_{(n-1)(n-2)} \cdots a_{32}a_{21}.$$

The fundamental braid admits many many braid transformations, in both the old and the new presentations, and so can be written in many ways as a positive word in the braid generators. As a result of this flexibility, it has two important properties:

(i) For any generator $a$, there exist $A, B \in B_n^+$ such that: $\mathbf{D} = aA = Ba$;

(ii) For each generator $a$ we have $a\mathbf{D} = \mathbf{D}\tau(a)$ and also $\mathbf{D}a = \tau^{-1}(a)\mathbf{D}$, where $\tau$ is the automorphism of $B_n$ which is defined by $\tau(\sigma_i) = \sigma_{n-i}$ for the old presentation and $\tau(a_{ts}) = a_{(t+1)(s+1)}$ for the new presentation.

(iii) $\tau(\{\mathbf{D}\}) = \{\mathbf{D}\}$.

2.3 There are partial orderings '$\geq$' and '$\leq$' in $B_n$. For two words $V$ and $W$ in $B_n$ we say that $V \geq W$ (resp. $W \leq V$) if $V = PW$ (resp. $V = WP$) for some $P \in B_n^+$. Note that $W$ is a positive word if and only if $W \geq e$. We denote $V < W$ (resp. $V > W$) if $V \leq W$ (resp. $V \geq W$) and $V \neq W$. In general $V \geq W$ is not equivalent to $W \leq V$, although if either $W$ or $V$ is a power of $\mathbf{D}$ the two ordering conditions are equivalent because powers of $\mathbf{D}$ commute with elements of $B_n$ up to powers of the index-shift automorphism $\tau$. Note that $\tau$ preserves the partial ordering.

2.4 The symbol $\mathbf{Q}$ denotes the set of all initial subwords of $\mathbf{D}$, and $\mathbf{Q}^\star = \mathbf{Q} \setminus \{e, \mathbf{D}\}$. The cardinality $|\mathbf{Q}_{old}|$ is $n!$, whereas the cardinality $|\mathbf{Q}_{new}|$ is the $n^{th}$ Catalan number. Note that $|\delta| < |\Delta|$, also $|\mathbf{Q}_{new}| < |\mathbf{Q}_{old}|$. These are the main reasons why it is sometimes easier to work with the new presentation than the old.

2.5 The *geodesic length* $l_Q(\{W\})$ was introduced and investigated by Ruth Charney in [2]. It is the smallest integer $k$ such that there is a word $q_1 q_2 \cdots q_k$ representing $\{W\}$, with each $q_i \in \mathbf{Q} \cup \mathbf{Q}^{-1}$. Define the geodesic length of the conjugacy class $l_Q([W])$ to be the shortest such representation for words in the conjugacy class $[W]$.

2.6 For each positive word $P$, there is a decomposition, called the *left-greedy decomposition*, $P = A_0 P_0$ for $A_0 \in \mathbf{Q}$ and $P_0 \geq e$, where $A_0$ has maximal length among all such decompositions, i.e. if $P = A_0' P_0'$, where $A_0' \in \mathbf{Q}$ and $P_0' \in B_n^+$, then $A_0' \leq A_0$. The term 'greedy' suggests that $A_0$ has absorbed as many letters from $P_0$ as it can without leaving $\mathbf{Q}$. The canonical factor $A_0$ is called the *maximal head* of $P$. If $P = A_0 P_0 = A_0' P_0'$ in left greedy form, then $\{A_0\} = \{A_0'\}$ and $\{P_0\} = \{P_0'\}$. (Remark: The term *left-canonical decomposition* was used in [1] and [3], however in recent years *left-greedy decomposition* has become the term of choice for the same concept in the literature, hence we now change our notation.)

2.7 Any word $W$ in the generators admits a unique *normal form* which solves the word problem in $B_n$. The normal form is:

$$W = \mathbf{D}^u A_1 A_2 \cdots A_k, \qquad u \in \mathbb{Z},\ A_i \in \mathbf{Q}^\star,$$

where for each $1 \leq i \leq k-1$, the product $A_iA_{i+1}$ is a left-greedy decomposition. The integer $u$ (resp. $u+k$) is called the *infimum* of $W$ (resp.*supremum* of $W$) and denoted by $\inf(W)$ (resp. $\sup(W)$).

2.8 To solve the conjugacy problem, we need to study the maximum and minimum values of inf and sup for the conjugacy class rather than for the word class. We consider the following two operations $\mathbf{c}$ and $\mathbf{d}$, called *cycling* and *decycling*, respectively. For a given braid in normal form $W = \mathbf{D}^u A_1 A_2 \cdots A_k$, we define:

$$\begin{aligned} \mathbf{c}(W) &= \mathbf{D}^u A_2 A_3 \cdots A_k \tau^{-u}(A_1) \\ \mathbf{d}(W) &= \mathbf{D}^u \tau^u(A_k) A_1 \cdots A_{k-1}. \end{aligned}$$

In general the braids on the right hand side will *not* be in normal form, and must be rearranged into normal form before the operation can be repeated.

2.9 **Theorem** (see [1, 3]):

(1) If $W$ is conjugate to $V$ and if $\inf(V) > \inf(W)$, then repeated cycling will produce $\mathbf{c}^\ell(W)$ with $\inf(\mathbf{c}^\ell(W)) > \inf W$.
(2) If $W$ is conjugate to $V$ with $\sup(V) < \sup(W)$, then repeated decycling will produce $\mathbf{d}^\ell(W)$ with $\sup(\mathbf{d}^\ell(W)) < \sup(W)$.
(3) The maximum value of inf and the minimum value of sup can be achieved simultaneously.

2.10 The *super summit set* $\mathrm{SSS}([W])$ ([1, 3]) is the set of all conjugates of $W$ which have the maximal infimum and the minimal supremum in the conjugacy class $[W]$. It is a proper subset of the *summit set* $\mathrm{SS}([W])$ which was introduced in by Garside in [4].

2.11 **Theorem** (see [1, 3, 7]): Let $W, W'$ be any two words in $\mathrm{SSS}([W] = \mathrm{SSS}([W'])$. Then there is a sequence

$$W = W_0 \to W_1 \to \cdots \to W_k = W'$$

such that each intermediate braid $W_i \in \mathrm{SSS}([W])$ and each $W_{i+1}$ is a conjugate of $W_i$ by a single member of $\mathbf{Q}$.

2.12 By the theorems in §2.9 and §2.11 one can compute $\mathrm{SSS}([W])$ as follows:

- Obtain an element $W'$ in the super summit set by iterating cyclings and decyclings, starting with any given word $W$.
- Compute the whole super summit set from $W'$ as follows: Compute $AW'A^{-1}$ for all $A \in \mathbf{Q}$ and collect the braids in the super summit set. Repeat the same process with each newly obtained element, until no new elements are obtained.

Therefore there is a finite time algorithm to generate $\mathrm{SSS}(W)$. This algorithm solves the conjugacy problem in $B_n$. The integers

$\inf([W])$ and $\sup([W])$ are the same for all members of $\mathrm{SSS}(W)$ and so are partial invariants of the conjugacy class $[W]$.

In this article, we obtain an upper bound for the necessary number of cyclings and decyclings in the theorem in §2.9 above. for both the old presentation and the new presentation. We denote the word length of $W$ by $|W|$. Our main result is:

**Theorem 1.** *Let $W \in B_n$. If $\inf(W)$ is not maximal for $[W]$, then $\inf(\mathbf{c}^{|\mathbf{D}|-1}(W)) > \inf(W)$. If $\sup(W)$ is not minimal for $[W]$, then $\sup(\mathbf{d}^{|\mathbf{D}|-1}(W)) < \sup(W)$.*

As immediate applications, we have:

**Corollary 2.** *Given any braid word $W \in B_n$, there is an algorithm which is polynomial in both word length and braid index for the computation of $\inf[W]$ and $\sup[W]$. Using the new presentation the complexity of the algorithm is $O(|W|^2n^2)$.*

**Corollary 3.** *There is an algorithm which is polynomial in both word length and braid index for the computation of the geodesic length $l_Q([W])$ of the conjugacy class of $W$, using either presentation. Using the new presentation the complexity is $O(|W|^2n^2)$.*

## 3. **Proof of Theorem 1 and Corollaries 2 and 3.**

**Proof of Theorem 1:** We focus on cycling because the proof and the difficulties are essentially identical for decycling.

Here is the plan of the proof. We begin with a word $W = \mathbf{D}^u P$ which is in normal form, so that $u = \inf(W)$ and $P > e$. By hypothesis $\inf([W]) > u$, so there exists an integer $m$ such that $u = \inf(W) = \inf(\mathbf{c}(W)) = \cdots = \inf(\mathbf{c}^m(W))$, but $\inf(\mathbf{c}^{m+1}(W)) > u$. Each instance of cycling can be realized by conjugation of $W$ by an element in $\mathbf{Q}^\star$, so we know there are $A'_1, A'_2 \ldots, A'_m \in \mathbf{Q}^\star \cup (\mathbf{Q}^\star)^{-1}$ such that after conjugating $W$, successively, by $A'_1, A'_2 \ldots, A'_m$ we obtain $W' = R'\mathbf{D}^u P(R')^{-1}$ with $\inf(W') = u + 1$. (See Lemma 4 below.) Write $R'$ in normal form. (See Lemmas 8 and 9.) Our plan is to show that the sequence of lengths of the canonical factors $H'_m, \ldots, H'_0$ for $R'$ satisfies $|H'_m| < |H'_{m-1}| < \cdots < |H'_0|$. Since each $H'_i \in \mathbf{Q}^\star$, we have $e < |H'_i| < |\mathbf{D}|$. This places a limit on the length of the chain, i.e. $m + 1 \leq |\mathbf{D}| - 1$ or $m \leq |\mathbf{D}| - 2$, as claimed.

We used the symbols $R', A'_i, H'_j$ in the description above, but in the actual proof we will use symbols $R, A_i, H_j$ which differ a little bit from

$R', A_i', H_j'$ because we wish to focus on the changes in the positive part $P$ of $W$, rather than on changes in $\mathbf{D}^u P$:

**Lemma 4.** *Choose any $W \in B_n$. Let $W = \mathbf{D}^u P$, where $u = \inf(W)$. Then $\inf([W]) > \inf(W)$ if and only if there exists a positive word $R$ such that $RP\tau^{-u}(R^{-1}) \geq \mathbf{D}$.*

*Proof.* By hypothesis $\inf([W]) > \inf(W)$, so there exists $X \in B_n$ with $\inf(XWX^{-1}) > \inf(W)$. Let $X = \mathbf{D}^v Y, Y \geq e$, where $v = \inf(Y)$. Then:

$$(\mathbf{D}^v Y)(\mathbf{D}^u P)(Y^{-1}\mathbf{D}^{-v}) \geq \mathbf{D}^{u+1},$$

which implies (via part (ii) of (3) above) that:

$$(\tau^u(Y))(P)(Y^{-1}) \geq \mathbf{D}.$$

Set $R = \tau^u(Y)$, so that $Y = \tau^{-u}(R)$. Then $R \geq e$ and

$$(R)(P)(\tau^{-u}(R^{-1})) \geq \mathbf{D},$$

as claimed. □

We will need to understand the structure of the positive word $R$ in Lemma 4, and to learn how the normal form of $R$ is related to that of $W$ and its images under repeated cycling. Once we understand all these issues, we will be able to extract information from $R$ about repeated cycling. We begin our work with several preparatory lemmas (i.e. Lemmas 5, 6 and 7.):

**Lemma 5.** *Suppose that $P \geq e$ and that $RP \geq \mathbf{D}$ for some $R \geq e$. Let $P = A_0 P_0$ be in left-greedy form. Then $RA_0 \geq \mathbf{D}$.*

*Proof.* See Proposition 3.9 (IV) of [1] for the new presentation and Proposition 2.10 of [3] for the old presentation. □

**Lemma 6.** *If $W \in B_n$ and $A \in \mathbf{Q}$, then $\inf(W) \leq \inf(WA) \leq \inf(W) + 1$.*

*Proof.* Since $W \leq WA \leq W\mathbf{D}$ and $\inf(W\mathbf{D}) = \inf(W) + 1$ the assertion follows. □

For each $A \in \mathbf{Q}$, let $\bar{A}$ denote the unique member of $\mathbf{Q}$ which satisfies $\bar{A}A = \mathbf{D}$.

**Lemma 7.** *Let $Z = B_\ell B_{\ell-1} \cdots B_1$ be the normal form for $Z \geq e$. Then $Z^{-1}\mathbf{D}^\ell \geq e$ and the normal form for $Z^{-1}\mathbf{D}^\ell$ is*

$$\tau(\bar{B}_1)\tau^2(\bar{B}_2)\cdots\tau^\ell(\bar{B}_\ell).$$

*Proof.* Observe that $\mathbf{D} = \bar{B}_i B_i$ implies that $\mathbf{D} = \tau^i(\bar{B}_i)\tau^i(B_i)$ for every $i = 1, \ldots, \ell$. Therefore:

$$\begin{aligned} Z^{-1}\mathbf{D}^\ell &= B_1^{-1}B_2^{-1}\cdots B_\ell^{-1}\mathbf{D}^\ell \\ &= (\mathbf{D}\tau(B_1^{-1}))(\mathbf{D}\tau^2(B_2^{-1}))\cdots(\mathbf{D}\tau^\ell(B_\ell^{-1})) \\ &= (\tau(\bar{B}_1)\tau(B_1)\tau(B_1^{-1}))(\tau^2(\bar{B}_2)\tau^2(B_2)\tau^2(B_2^{-1}))\cdots(\tau^\ell(\bar{B}_\ell)\tau^\ell(B_\ell)\tau^\ell(B_\ell^{-1})) \\ &= \tau(\bar{B}_1)\tau^2(\bar{B}_2)\cdots\tau^\ell(\bar{B}_\ell) \end{aligned}$$

because

$$\tau(B_i)\tau(B_i^{-1}) = \tau(B_iB_i^{-1}) = \tau(e) = e.$$

□

We continue the proof of Theorem 1. By §2.8 and Lemma 6 there exists a nonnegative integer $m$ such that $\inf(\mathbf{c}(W)) = \inf(\mathbf{c}^2(W)) = \cdots = \inf(\mathbf{c}^m(W))$ but $\inf(\mathbf{c}^{m+1}(W)) = \inf(W) + 1$. To prove Theorem 1, we must show that $m+1$ is bounded above by $|\mathbf{D}| - 1$. Let $W = \mathbf{D}^u P$, where $P \geq e$ and $u = \inf(W)$. By Lemma 4 we know that $\inf([W]) > \inf(W)$ if and only if there exists a positive word $R$ such that $RP\tau^{-u}(R^{-1}) \geq \mathbf{D}$. Assume that among all such words we have chosen $R$ so that $|R|$ is minimal. We wish to describe this shortest word $R$ as a specific product (in general not left-greedy) of canonical factors. Our first observation is:

**Lemma 8.** $\inf(R) = 0$.

*Proof.* If not, then $R = \mathbf{D}R'$ for some $R' \geq e$ and

$$R'P\tau^{-u}(R')^{-1} = \mathbf{D}^{-1}RP\tau^{-u}(R)^{-1}\mathbf{D} = \tau(RP\tau^{-u}(R)^{-1}) \geq \mathbf{D},$$

which contradicts the minimality of $|R|$. □

**Lemma 9.** *Let $\mathbf{c}^i(W) = \mathbf{D}^u A_i P_i$, where $A_i$ is the maximal head of $\mathbf{c}^i(W)$. Then the positive word $R$ whose existence is guaranteed by Lemma 4 is related to the $A_i$'s as follows:*

$$R = \tau^{-m}(\bar{A}_m)\cdots\tau^{-1}(\bar{A}_1)\bar{A}_0.$$

*Proof.* Our starting point is:

$$RP\tau^{-u}(R)^{-1} \geq \mathbf{D},$$

which implies that $RP \geq \mathbf{D}$. Since $P = A_0P_0$ is left-greedy, Lemma 5 then implies that $RA_0 \geq \mathbf{D}$ and so $R = R_1\bar{A}_0$ for some positive word $R_1$. Now:

$$\begin{aligned} RA_0P_0\tau^{-u}(R)^{-1} &= R_1\bar{A}_0A_0P_0\ \ \tau^{-u}(\bar{A}_0^{-1})\tau^{-u}(R_1^{-1}) \\ &= R_1\mathbf{D}P_0\tau^{-u}(A_0)\mathbf{D}^{-1}\tau^{-u}(R_1^{-1}) \\ &= R_1\tau^{-1}\left(A_1P_1\right)\tau^{-u}(R_1^{-1}). \end{aligned}$$

Since $RA_0P_0\tau^{-u}(R^{-1}) \geq \mathbf{D}$, we conclude that:

$$R_1\tau^{-1}(A_1P_1)\tau^{-u}(R_1^{-1}) \geq \mathbf{D}.$$

Iterating the construction, we obtain $R_1 = R_2\tau^{-1}(\bar{A}_1)$ for some positive word $R_2$, also $R_2 = R_3\tau^{-2}(\bar{A}_2), \ldots, R_m = R_{m+1}\tau^{-m}(\bar{A}_m)$. Putting all of these together we learn that:

$$R = R_{m+1}\tau^{-m}(\bar{A}_m)\cdots\tau^{-1}(\bar{A}_1)\bar{A}_0$$

for some positive word $R_{m+1}$. Let $S = \tau^{-m}(\bar{A}_m)\cdots\tau^{-1}(\bar{A}_1)\bar{A}_0$, so that $R = R_{m+1}S$. A straightforward calculation shows that

$$\tau^{-(m+1)}(SP\tau^{-u}(S^{-1})) = A_{m+1}P_{m+1}.$$

Since $\inf(\mathbf{c}^{m+1}(W)) = \inf(W) + 1$, we have

$$1 = \inf(\tau^{-(m+1)}(SP\tau^{-u}(S^{-1}))) = \inf(SP\tau^{-u}(S^{-1})).$$

By the minimality of $|R|$, we must have $R = S$. Lemma 9 is proved. □

The expression given for $R$ in the statement of Lemma 9 is in general not in normal form. We now study the maximal head $H_0$ of $R = \tau^{-m}(\bar{A}_m)\cdots\tau^{-1}(\bar{A}_1)\bar{A}_0$, and related canonical factors $H_1, \ldots, H_m$. To define them, let $H_k$ be the maximal head of $\tau^{-m}(\bar{A}_m)\cdots\tau^{-k}(\bar{A}_k) \subset R$.

**Lemma 10.** $e < H_m < H_{m-1} < \cdots < H_1 < H_0 < \mathbf{D}$.

*Proof.* Our first observation is that $\inf(R) = 0$ (see Lemma 8). Since $H_0$ is the maximal head of $R$, it follows that

$$H_0 < \mathbf{D}.$$

Our second observation is that by hypothesis $\inf(\mathbf{c}^m(W)) = u$ and $\mathbf{c}^m(W) = \mathbf{D}^u A_m P_m$ is left-greedy, so that $A_m < \mathbf{D}$, which implies that $e < \bar{A}_m$ and so:

$$e < H_m.$$

Our third observation is that by the definition of $H_k$ we must have:

$$H_m \leq H_{m-1} \leq \cdots \leq H_1 \leq H_0.$$

Therefore the only thing that we need to prove is that $H_{k+1} \neq H_k$ for $k = 0, 1, \ldots, m-1$.

We first prove the assertion for $k = 0$. Assume that $H_1 = H_0$. We will show that this leads to a contradiction to our choice of $R$.

We are given that:

$$R = \tau^{-m}(\bar{A}_m)\cdots\tau^{-1}(\bar{A}_1)\bar{A}_0 = B_\ell B_{\ell-1}\cdots B_1,$$

where the decomposition on the left comes from Lemma 9 and the one on the right is the normal form for $R$. By Lemma 7 the normal form for $R^{-1}\mathbf{D}^\ell$ is $\tau(\bar{B}_1)\tau^2(\bar{B}_2)\cdots\tau^\ell(\bar{B}_\ell)$.

By hypothesis $H_1 = H_0 = B_\ell$, so

$$\tau^{-m}(\bar{A}_m)\cdots\tau^{-1}(\bar{A}_1) = B_\ell R_1$$

for some $R_1 \geq e$. Since $B_\ell R_1 \bar{A}_0 = R = B_\ell B_{\ell-1}\cdots B_1$, it follows that $B_{\ell-1}\cdots B_1 = R_1\bar{A}_0$ and so

$$B_{\ell-1}\cdots B_1 P \geq \mathbf{D}.$$

Let $a_i$ be the infimum of $B_{\ell-1}\cdots B_1 P\tau^{-u}\left(\tau(\bar{B}_1)\tau^2(\bar{B}_2)\cdots\tau^i(\bar{B}_i)\right)$. Then

1. $a_0 \geq 1$ by the above discussion,
2. $a_i \leq a_{i+1} \leq a_i + 1$ by Lemma 5, and
3. if $a_i = a_{i+1}$, then $a_i = a_{i+1} = \cdots = a_\ell$ since $\tau^i(\bar{B}_i)\tau^{i+1}(\bar{B}_{i+1})$ is left-greedy.

If $a_{\ell-1} \geq \ell$, then

$$(B_{\ell-1}\cdots B_1)P\tau^{-u}(B_{\ell-1}\cdots B_1)^{-1} \geq \mathbf{D},$$

which contradicts the minimality of $|R|$. So $a_{\ell-1} \leq \ell - 1$. Then $a_i = a_{i+1}$ for some $i \leq \ell - 2$ and so $a_i = a_{i+1} = \cdots = a_\ell \leq \ell - 1$ so that $\inf(RP\tau^{-u}(R^{-1})) \leq 0$. However, by our choice of $R$, we know that $\inf(RP\tau^{-u}(R^{-1})) > 0$. Retracing our steps we conclude that the assumption $H_1 = H_0$ is impossible, so $H_1 < H_0 < \mathbf{D}$.

It remains to attack the cases $k > 0$. The method is identical to the case $k = 0$. Set $V = \mathbf{c}^k(W) = \mathbf{D}^u A_k P_k$ and let $V$ play the role of $W = \mathbf{D}^u A_0 P_0$. □

The proof of Theorem 1 is almost complete. We have learned that $e < H_m < H_{m-1} < \cdots < H_1 < H_0 < \mathbf{D}$. This implies that:

$$0 < |H_m| < |H_{m-1}| < \cdots < |H_1| < |H_0| < |\mathbf{D}|.$$

Thus the length $m+1$ of the chain must be smaller than $|\mathbf{D}|$, that is $m + 1 \leq |\mathbf{D}| - 1$. The proof of Theorem 1 is complete. □

**Proof of Corollary 2:** The proof follows directly from Theorem 1 and the estimates in [1]. In Theorem 4.4 of [1] it is shown that for the new presentation there is an algorithm rewriting a word into its left greedy form that is a $O(|W|^2 n)$ solution to the word problem. The initial preparation of our algorithm puts a given word $W$ into its left greedy form and takes $O(|W|^2 n)$. Notice that the number of factors is proportional to $|W|$ in the worst case. In order to compute inf we need to cycle at most $n-2$ times. After each cycling the new word so-obtained must be put into left greedy form but this time it takes only

$O(|W|n)$ by Corollary 3.14 of [1]. Thus the test to determine whether inf is maximal takes $O(|W|n^2)$. If it is not the entire process must be repeated, but the number of such repeats, i.e., the total increase of inf, is clearly bounded by the number of factors so the entire calculation is $O(|W|^2n^2)$. We note that if $W$ is a positive word, the total increase of inf is the maximum number of powers of $\delta$ formed cyclically from $W$ but this number is clearly bounded by $|W|/(n-1)$, so the entire calculation is $O(|W|^2n)$. The discussion for the old presentation is similar and is left to the reader. □

**Proof of Corollary 3:** Let $W = \mathbf{D}^u A_1 A_2 \cdots A_k$ be a word which is in normal form and which realizes the maximum value $u$ of inf and the minimum value $k$ of sup for the word class $\{W\}$. The geodesic length $l_Q(\{W\})$ of $\{W\}$ is computed in [2] (or see [8]) as follows:

(i) If $u \geq 0$ then $W$ is a positive word of geodesic length $l_Q(\{W\}) = u + k$.

(ii) If $-k \leq u < 0$, then we may use the fact that for every $X_i \in \mathbf{Q}$ there exists $Y_i \in \mathbf{Q}$ with $X_iY_i = \mathbf{D}$. From this it follows that $\mathbf{D}^{-1}X_i = Y_i^{-1}$. Using the additional fact that if $\tau$ is the index shift automorphism of §2.2, then $\tau(\mathbf{Q}) = \mathbf{Q}$, it follows that we may eliminate all of the powers of $\mathbf{D}$ and replace $u$ of the factors $A_1, A_2, \ldots A_u \in \mathbf{Q}$ with appropriate elements of $\mathbf{Q}^{-1}$, thereby achieving a shorter word. So in this case $l_Q(\{W\}) = k$.

(iii) If $u < -k$ then every factor $A_1, A_2, \ldots A_u \in \mathbf{Q}$ is replaced by an appropriate element of $\mathbf{Q}^{-1}$. After all of these reductions the new word will be entirely negative. Its geodesic length is $l_Q(\{W\}) = -u$.

(iv) The three cases may be combined into a single formula: $l_Q(\{W\}) = max(k + u, -u, k)$.

The above considerations relate to the length of a word class $\{W\}$. However, observe that the normal form for elements in the conjugacy class $[W]$ is identical to that for the word class, moreover if $Y, Z$ are in the super summit set of $[W]$ then $\inf(Y) = \inf(Z)$ and $\sup(Y) = \sup(Z)$. Since the complexity of computing $l_Q([W])$ is identical to the complexity of computing $\inf([W])$ and $\sup([W])$, the assertion then follows from Corollary 2. □

## 4. **Are the cycling-decycling bounds sharp?**

Note that the bound we obtained for the number of cyclings and decyclings in Theorem 1 is $n - 2$ for the new presentation and $-1 +$

$(n-1)(n-2)/2$ for the old presentation. In this section we investigate whether these bounds are sharp.

We first give an example of $n$-braid written in the new generators for which $n-2$ cyclings are required to increase the infimum. This shows that the bound given in Theorem 1 is sharp for the new presentation. To simplify notation, use $[t, t-1, \dots, s]$ instead of $a_{t(t-1)}a_{(t-1)(t-2)}\cdots a_{(s+1)s}$. Consider the example $W = ([2,1][5,4,3])([3,2])$ in normal form. Then

$$\begin{aligned}
\mathbf{c}(W) &= ([3,2])([2,1][5,4,3]) = ([3,2,1][5,4])([4,3]) \\
\mathbf{c}^2(W) &= ([4,3])([3,2,1][5,4]) = ([4,3,2,1])([5,4]) \\
\mathbf{c}^3(W) &= ([5,4])([4,3,2,1]) = [5,4,3,2,1] = \delta
\end{aligned}$$

So $\inf(W) = \inf(\mathbf{c}(W)) = \inf(\mathbf{c}^2(W)) = 0$ but $\inf(\mathbf{c}^3(W)) = 1$. More generally, if

$$W = [2,1][n, n-1, \dots, 3, 2] = ([2,1][n, n-1, \dots, 3])([3,2]),$$

then $\inf(W) = \inf(\mathbf{c}^{n-3}(W)) = 0$ but $\inf(\mathbf{c}^{n-2}(W)) = 1$. See Figure 1(a) for a sketch of the braid $W$ in the case $n = 7$.

In the old presentation, the example in [3] shows that $\inf(W) = \inf(\mathbf{c}(W)) = 0$ but $\inf(\mathbf{c}^2(W)) = 1$. There are plenty of examples for which more than 2 cyclings are required to increase the infimum. Let $(a_1, \dots, a_n)$ denote the permutation braid corresponding to the permutation $\pi$ on $\{1, \dots, n\}$ defined by $\pi(i) = a_i$, Consider the following example, with $W \in B_{2k+1}$.

$$W = (\underbrace{2k+1, 2k, \dots, 3}_{2k-1}, 1, 2)(\underbrace{1, 2, \dots, k}_{k}, \underbrace{k+2, \dots, 2k+1}_{k}, k+1)$$

Then $\inf(W) = \inf(\mathbf{c}^{2k-1}(W)) = 0$ but $\inf(\mathbf{c}^{2k}(W)) = 1$. See Figure 1(b) for a sketch of this example in the case $n = 7$.

For another example let $W \in B_{2k+1}$ be such that

$$\begin{aligned}
W = (&\underbrace{2k+1, \dots, k+3}_{k-1}, k+1, k+2, \underbrace{k, k-1, \dots, 1}_{k}) \\
&(\underbrace{3, 4, \dots, k+1}_{k-1}, 1, \underbrace{k+2, \dots, 2k}_{k-1}, 2, 2k+1)
\end{aligned}$$

See Figure 1(c). Then $4k-5$ cyclings are needed to increase the infimum. So if $n$ is odd, there is an example for which $2n-7$ cyclings are needed. Therefore the lower bound for the old presentation is at least linear in $n$.

We do not know an exact bound that works for every $n$-braid written in the old generators. It is easy to see that the upper bound in $B_3$ is 1, that is, if $\inf(W) = \inf(\mathbf{c}(W))$ for $W \in B_3$, then the infimum is already

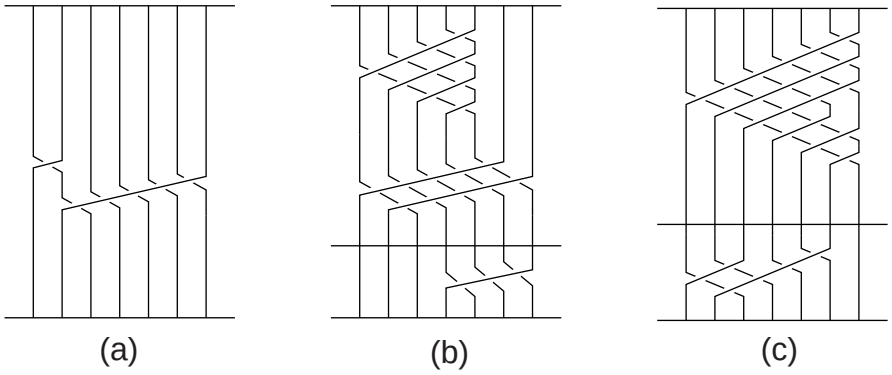


FIGURE 1. Examples

maximized. In an exhaustive search, we learned that the upper bound for $B_4$, using the old presentation, is 2 for positive words whose normal form contains up to 5 canonical factors.

## 5. **Complexity issues and the conjugacy problem**

In this section we consider implications of the work in the preceding sections for the complexity of the conjugacy problem in $B_n$.

5.1. **The special cases $n = 3$ and 4:** Before discussing the problem, it will be helpful to review what is known about the cases $n = 3$ and 4, since well-chosen examples always help one to arrive at a better understanding of a problem. In the manuscript [8] P.J. Xu introduced the new presentation for $B_3$ and used it to solve the word and conjugacy problems in $B_3$ and to study the letter lengths of shortest words in a word and conjugacy class in $B_3$, using the new presentation. Her main result in this regard was that words of shortest 'geodesic length' (she doesn't use the term geodesic length, which was introduced after she completed her work) are, without further work, also words of shortest letter length in the new generators. She also found growth functions for $B_3$, both for word classes and conjugacy classes, proved that they were rational, and computed the rational functions which described them. Her algorithm for the conjugacy problem was clearly polynomial in $|W|$.

In [5] the word and conjugacy problems were solved in $B_4$, using the new presentation and following the methods of [8]. The authors also solved the shortest word problem in conjugacy classes. In a forthcoming paper the second and third author of this paper will prove that the algorithm for the conjugacy problem in [5] is polynomial in $|W|$.

5.2. **The conjugacy problem:** In §2.10 above the super summit set $\mathrm{SSS}([W])$ of the conjugacy class of $W \in B_n$ is defined. It is a finite set and it can be computed in a systematic manner in a finite number of steps from any braid word $W$ which realizes $\inf([W])$ and $\sup([W])$. The Theorem which is quoted in §2.11 above asserts that $W$ is conjugate to $V$ in $B_n$ if and only if $\inf([W]) = \inf([V])$, $\sup([W]) = \sup([V])$ and $\mathrm{SSS}([W]) = \mathrm{SSS}([V])$.

The super summit set has a fairly transparent structure when $n = 3$, the main reason being that words in $\mathbf{Q}^\star = \mathbf{Q} \setminus \{\delta, e\}$ all have length 1. In $B_4$ the situation is a little bit more complicated, but still within reach. Let $W = \delta^u A_1 A_2 \cdots A_k$ be in the super summit set of $[W]$ and be in normal form, and let $A = A_1 A_2 \cdots A_k$ be the 'positive part' of $W$. Notice that $\delta$ has letter length 3 and the $A_j's$ are elements of $\mathbf{Q}^\star$, and so have letter length 1 or 2. Let $k_1$ (resp. $k_2$) be the number of factors in $A$ which have length 1 (resp. 2). Let $e$ be the exponent sum of $W$. Clearly $e$ is a class invariant. Since $k = k_1 + k_2$ and since $e = 3u + k_1 + 2k_2$ it follows that $k_1$ and $k_2$ are determined by the triplet $(u = \inf, k = \sup, e)$. This makes the SSS somewhat easier to understand in the case $n = 4$ than in the general case.

In the general case the super summit set $\mathrm{SSS}([W])$ splits into orbits under cycling and decycling. Clearly the number of such orbits and their sizes are class invariants, but unfortunately we have examples to show that they are not complete invariants. The orbits are complicated by the fact that $\mathbf{Q}^\star$ contains elements of letter length $1, 2, \ldots, n-2$, and the number $k_i$ of elements of letter length $i$ of a member of $\mathrm{SSS}([W])$ is no longer controlled by $(u, k, e)$. We don't know whether $k_1, \ldots, k_{n-2}$ are orbit invariants, and if they can vary from one orbit to another. Also, while it is known that one can pass from any orbit to any other orbit by conjugating by an appropriate product of elements of $\mathbf{Q}$, it is difficult to understand which products do the job. While the super summit set is a great improvement over the summit set of [4], it is still too big to make it possible to study many examples. For all these reasons the complexity of the conjugacy problem remains open at this time. Nevertheless, based on what we know, we conjecture:

**Conjecture 11.** *There is an algorithmic solution to the conjugacy problem in $B_n$, using the combinatorial approach which is described in this paper, which is polynomial in word length $|W|$ for each fixed braid index $n$.*

## References

[1] J. S. Birman, K. H. Ko and S. J. Lee, *A new approach to the word and conjugacy problem in the braid groups*, Advances in Mathematics, **139** (1998), 322-353.

[2] R. Charney, *Geodesic automation and growth functions for Artin groups of finite type*, Math. Ann. **301** (1995), 307-324.

[3] E. A. Elrifai and H. R. Morton, *Algorithms for positive braids*, Quart. J. Math. Oxford, **45** (1994), 479–497.

[4] F. A. Garside, *The braid group and other groups*, Quart. J. Math. Oxford, **20** (1969), 235–254.

[5] E. S. Kang, K. H. Ko and S. J. Lee, *Band-generator presentation for the 4-braid group*, Topology Appl. **78** (1997), 39–60.

[6] D. Krammer, *The braid group $B_4$ is linear*, Inventiones Mathematica, to appear.

[7] W. Thurston, *Finite state algorithms for the braid group*, Chapter 9 of 'Word processing in groups', D. B. A. Epstein, J. W. Cannon, D. F. Holt, S. V. F. Levy, M. S. Patterson and W. Thurston. Jones and Bartlett, Boston and London (1992).

[8] P.J. Xu, *The genus of closed 3-braids*, J. Knot Theory and its Ramifications **1**,no. 3 (1992), 303-326.

Department of Mathematics, Barnard College of Columbia University, 2990 Broadway, New York, NY 10027-4427

*E-mail address*: jb@math.columbia.edu

Department of Mathematics, Korea Advanced Institute of Science and Technology, Taejon, 305–701, Korea

*E-mail address*: {knot, sjlee}@knot.kaist.ac.kr